LEES MEER OP: **WWW.TOPICNEDERLAND.NL**

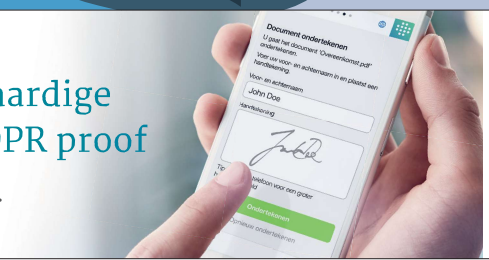
VEILIGHEID & INDUSTRIE 4.0

Nederlandse industrie staat er goed voor na uitzonderlijk jaar

Een veiliger Nederland vraagt om alertheid en maatregelen met impact

Digitaal ondertekenen met hoogwaardige identiteitsverificatie en volledig GDPR proof

Probeer het nu kosteloos en vrijblijvend bij dé marktleider.



Scan de QR code en maak een gratis account aan

evidos EVIDENCE IN ONLINE SERVICES

Profielinterview Petra Oldengarm, Cyberveilig Nederland

Goede cybersecurity begint met nadenken o

De vraag die elke ondernemer en organisatie zich moet stellen, luidt: hoe afhankelijk ben ik van mijn digitale systemen? "Ik denk dat veel ondernemers zich díe vraag nog onvoldoende stellen. Hoe lang kan ik doorgaan zonder mijn data? Als dat hooguit een uur is, moet je een andere investering doen in je veiligheid dan wanneer het een paar dagen zonder ook wel lukt," waarschuwt directeur van Cyberveilig Nederland Petra Oldengarm. Aanvallers zitten vaak al maanden in het ICT-systeem voordat het daadwerkelijke effect ervan zichtbaar wordt.

De Nederlandse samenleving is zich onvoldoende bewust van de digitale afhankelijkheid, meent Oldengarm. "Dat bewustzijn, en dat roepen we al jarenlang, is nog steeds niet groot genoeg." Als voorbeeld gebruikt Oldengarm een recente ervaring op een postkantoor om de digitale kwetsbaarheid te illustreren. "Er was een pakketje uit de VS voor mij binnengekomen. Het digitale systeem lag eruit. Ik kreeg de zending niet mee omdat de medewerker niet in staat was om te registreren dat ik het pakje had aangenomen. Dan zie je dat er geen back-up plan is bedacht voor als je systemen het niet doen. Uiteindelijk heb ik een week op mijn pakketje moeten wachten." Haar boodschap: je moet je niet alleen richten op preventie, maar ook zorgen dat je dreigingen snel detecteert en er adequaat op kunt reageren.

OMT voor cybercrisissen

"We hebben in toenemende mate te maken met allerlei aanvallen, inbraken en spionageachtige zaken. De recente ophef over het lek in de Microsoft Exchange server laat zien dat we ons moeten blijven voorbereiden op nieuwe aanvallen, de komende jaren. Dat betekent dat weerbaarheid net zo belangrijk, zo niet belangrijker is dan het al was." Beveiliging van het eigen ICT-systeem begint met simpele vragen over businesscontinuïteit, benadrukt Oldengarm. "Het is belangrijk te erkennen dat werk meer en meer afhankelijk is van digitale systemen en veiligheid daarmee hand in hand gaat. Wij roepen vanuit de cybersecuritysector al jarenlang vanaf de zijlijn: ga aan de slag!" "De focus ligt historisch gezien nog veel op het voorkomen van cyberincidenten. Tegelijkertijd moeten organisaties de aandacht verplaatsen naar de vraag: hoe zorg ik dat ik een incident zo snel mogelijk ontdek, om de schade te beperken? En ook: hoe los ik een incident zo snel mogelijk weer op, als ik het ontdek? Organisaties moeten hun governance op orde hebben. Het is zaak dat je je op boardroom- en directieniveau druk maakt over digitale veiligheid en dat je daar mensen verantwoordelijk voor maakt."

PETRA OLDENGARM, DIRECTEUR CYBERVEILIG NEDERLAND

©Arenda Oomen Fotografie

"Een aanval detecteren en een goede respons organiseren zijn twee belangrijke aandachtspunten." Ze maakt de vergelijking met de coronapandemie: "Wat als we worden getroffen door een digitaal virus? We kunnen leren van de aanpak van de

Digitale veiligheid is een onderdeel van de businesscontinuïteit.

NFIR

IT FORENSICS & INCIDENT RESPONSE

Managed Detection & Response

Detecteer digitale dreigingen in uw ICT infrastuctuur om adequaat te kunnen reageren

www.nfir.nl

Security Monitoring | Incident Response | Digitaal Forensisch Onderzoek | Pentesten | Security Awareness

over de eigen businesscontinuïteit

coronacrisis en lessen trekken van wat wel en wat niet heeft gewerkt. We hebben de overheid geadviseerd om een OMT voor cybercrisissen in te richten, om beter voorbereid te zijn op een groot incident of crisis."

Openheid

De cyberinbraak bij de gemeente Hof van Twente – waarbij hackers binnendrongen via het simpele wachtwoord Welkom2020 – benadrukt het belang van veilige wachtwoorden, maar vooral ook van oplossingen waardoor de afhankelijkheid van en kwetsbaarheid voor wachtwoorden vermindert. Gelukkig zie je steeds meer oplossingen als tweefactor-authenticatie. Oldengarm benadrukt het toenemende belang van informatiedeling, zoals in het geval van Hof van Twente, maar ook bij de cyberaanval op de Universiteit van Maastricht. "Ze hebben daar het goede voorbeeld in gegeven. Tussen de universiteiten onderling is informatie gedeeld, waardoor ze zich nu gezamenlijk beter kunnen beschermen tegen cyberaanvallen." Oldengarm is blij met die openheid. "Het is belangrijk om informatie met elkaar te delen. Dat gebeurt gelukkig op steeds grotere schaal." Ze vergelijkt het met de klassieke, fysieke inbraak. "Als ik weet dat bij mijn buurman de deur is opengebroken met een kerntrekmethode, dan laat ik daarna zo snel mogelijk een anti-kerntrekslot op mijn deur monteren. Zo werkt het in het cyberdomein ook. Als je weet hoe aanvallers te werk gaan, kan je je preventie-, detectie- en responsmaatregelen verbeteren en adequater optreden als er iets misgaat."

Teken van kracht

Minder blij is Oldengarm met het feit dat organisaties en bedrijven die slachtoffer worden van een cyberincident aan de schandpaal worden genageld. "Een recent voorbeeld is het datalek bij de GGD. Het is terecht dat je je afvraagt of de organisatie voldoende maatregelen heeft getroffen. Die vraag moet je sowieso blijven stellen. Aan de andere kant is het zo dat je, als je met de vinger blijft wijzen, organisaties schuw maakt om naar buiten te treden na een cyberaanval of diefstal van gevoelige data. Ik denk dat we juist toe moeten naar een situatie waarbij het publiceren en bekendmaken van cyberincidenten juist

"We hebben de overheid geadviseerd om een OMT voor cybercrisissen in te richten."

wordt gezien als een kracht. En dat het stilhouden daarvan reputatieschade moet opleveren. Zover zijn we helaas nog niet."

Impact voor ondernemer

Het Digital Trust Center van de overheid helpt kleinere ondernemingen bij hun cyberveiligheid en de huidige wetgeving verplicht met name digitale providers en vitale organisaties om een minimum set aan beveiligingsmaatregelen te nemen. "Het is zaak om er zo snel mogelijk achter te komen dat een aanvaller in je systeem zit," benadrukt Oldengarm. Ze verwijst naar een rapport van IBM, dat een datalek gemiddeld pas na 60 dagen wordt ontdekt. Gemiddeld zitten hackers drie tot zes maanden in een systeem voordat de daadwerkelijke aanval plaatsvindt. "Dat betekent dat je als organisatie al maandenlang slachtoffer bent, zonder dat je het doorhebt." Ze maakt opnieuw een vergelijking met beveiligingsmaatregelen die je treft in het fysieke domein: "Beveiliging is bedoeld om te voorkomen dat iemand binnenkomt. Je kunt een slot op je deur zetten, maar je kunt ook een beveiligingscamera of bewaking neerzetten om te controleren wie binnenloopt en of er misschien iemand binnenloopt die daar niet hoort. Dat geldt ook voor het digitale domein: als een hacker toch is binnengedrongen, is het belangrijk dat je zo snel mogelijk doorhebt, dat iemand in het systeem zit. Dat betekent dat je de detectie op orde moet brengen.

De aanvallen worden geavanceerder, waarschuwt Oldengarm. "Tegenwoordig zie je dat een digitale inbraak vaak aan de digitale gijzeling van gegevens voorafgaat en kwaadwillenden op zoek gaan naar welke systemen ze moeten versleutelen. Als je pech hebt, is dat inclusief al je back-ups. Zeker bij kleinere bedrijven kan de impact groot zijn. Als je al je technische tekeningen in je ICT-systeem hebt staan, je klantgegevens en ga zo maar door, kan de schade van zo'n aanval enorm zijn en uiteindelijk leiden tot een faillissement. En de psychische impact van een aanval voor de ondernemer zelf is vaak groot. Het lijkt simpel, zo'n aanval, maar waaiert uit naar zoveel meer qua impact."

Checklist digitale kwetsbaarheid

Cyberveilig Nederland heeft samen met diverse samenwerkingspartners een risicoclassificatie ontwikkeld waarmee kleinere ondernemingen met een elftal vragen eenvoudig kunnen inschatten hoeveel risico ze lopen en welke beveiligingsmaatregelen ze op grond van hun classificatie minimaal moeten nemen. Het is een concrete tool die bedrijven kunnen gebruiken.

www.digitaltrustcenter.nl/risicoklasse

IN SAMENWERKING MET VICTA BUSINESS INTELLIGENCE

Data-analytics: welke inzichten schuilen er in jouw data?

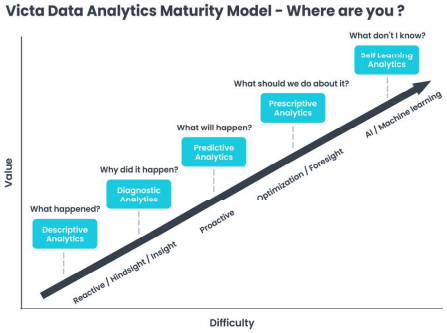
Start vandaag nog met het maken van data-gestuurde beslissingen.

Op basis van data kun je reageren, acteren en vooruitblikken. "Ons ultieme doel is om bedrijven data-gestuurd te maken," vertelt oprichter en eigenaar Carlo Vruwink. "Slim toepassen van data helpt bij het nemen van betere, zakelijke beslissingen."

"Bedrijven beschikken over een tsunami aan databronnen, van HRM en recruitment tot marketing, financieel, productie en IoT-data. "Veel organisaties gebruiken deze informatie vooral om terug te kijken: wat is er gebeurd? Terwijl ze op een schat aan informatie zitten die relevant kan zijn en kan helpen bij de vragen: waarom is het gebeurd? Wat gaat er gebeuren?"

Openbare databronnen

Victa Business Intelligence helpt bedrijven om data om te zetten in klinkende munt. Als voorbeeld noemt Vruwink de invloed van het weer op de omzet of planning van de winkels. "Het weer is een openbare databron. Van het KNMI kun je tot jaren terug data krijgen. Die koppelen we aan de data van de klant om ze te helpen met voorspellingen over de dagomzet, personeelsbezetting of inkoop. Als je datasets op de juiste manier koppelt en analyseert, leidt dat tot slimmere, data-gestuurde beslissingen."



Victa levert al ruim tien jaar innovatieve business intelligenceoplossingen aan meer dan 800 bedrijven.

Data-geletterdheid

"We genereren inzicht en helpen onze klanten om betere, data-gestuurde beslissingen te nemen." Dat laatste is een proces, benadrukt Vruwink. "Je organisatie moet er klaar voor zijn. Dat zien we nog wel eens misgaan. Al maken we nog zo'n mooi dashboard, het is aan de organisatie om geld te verdienen met die informatie. Daarom leveren we niet alleen de softwareoplossingen, maar doen we ook de support, consultancy en opleidingen erbij. We proberen mensen data-geletterd maken. Ze bewust te maken van de waarde van data."

VICTA BUSINESS INTELLIGENCE

>> Kijk voor meer informatie over dataoplossingen op **www.victa.nl**